4T

УДК 681.3:519

А.Н. Терещенко
Институт кибернетики им. В.М. Глушкова НАН Украины, г. Киев
teramidi@ukr.net

Оптимизация метода Питасси вычисления свертки

Предложенный метод расширяет диапазон используемых разрядностей циклической свертки за счет применения эффективного метода вычисления циклической свертки разрядностью 2*K*, где *K* – нечетное. Показано, что для вычисления свертки такой разрядности достаточно вычислить только две свертки половиной (от начальной) разрядности, при большем количестве пред- и поствычислений в виде циклических сдвигов по сравнению с методом Питасси. Представлены в общем виде формулы вычисления циклической свертки. Приведена реализация операции многоразрядного умножения на основе циклической свертки. В виде таблицы приведены оценки сложности вычисления свертки большой разрядности вида $N = K \cdot 2^n$, $n > 1$ для $K = 3,5,7,9$.

Введение

В последнее время большее внимание уделяется вопросам цифровой обработки сигналов и методам оптимизации вычислений, связанных с этой обработкой [1-6]. В статье особое внимание уделяется методам вычисления циклической свертки, которая широко применяется в построении цифровых фильтров, асимметричной криптографии и т.д. Как известно, выбор метода зависит от его области эффективного использования. Циклическая свертка применяется при реализации быстрой операции умножения. Операция умножения занимает большую часть вычислительного времени в операциях асимметричной криптографии, таких, как генерация и распределение секретного ключа, шифрование и дешифрование информации, проверка и наложение цифровой подписи и т.д.

Целью данной статьи является оптимизация вычисления свертки. Основное внимание уделяется уменьшению сложности алгоритма за счет уменьшения числа вычислений сверток меньшей разрядности. В данной работе приводится применение циклической свертки для реализации операции умножения. Как известно, эффективность операции умножения больших чисел зависит от метода реализации, а точнее, от количества операций умножения однократной точности, поэтому основной целью статьи является уменьшение общего числа операций умножений.

Ниже описан метод, при котором для вычисления свертки разрядностью 2*K*, где *K* – нечетное, достаточно вычислить 2 свертки разрядностью *K*. Приведем вначале эффективный алгоритм вычисления свертки разрядностью 2*K*, где *K* – четное, предложенный Питасси, который требует вычисления 3 сверток меньшей разрядности на всех итерациях.

Операторы и условные обозначения

Последовательности разрядности N могут быть представлены в виде векторов: $\overline{x} = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{bmatrix}$, $\overline{y} = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{bmatrix}$.

Циклическую свертку двух последовательностей $\overline{x}$ и $\overline{y}$ обозначим оператором $\otimes$:

$$\overline{r} = \overline{x} \otimes \overline{y}\,,\ \overline{r} = (r_0 ... r_{N-1})\,, r_k = \sum_{p=0}^{N-1} x_p y_{(p+k) \bmod N}\,,\ k = \overline{0, N-1}\,,$$

что равносильно записи:

$$\begin{array}{c|cccc} x_0 & y_0 & y_1 & y_2 & y_3 \\ x_1 & y_1 & y_2 & y_3 & y_0 \\ x_2 & y_2 & y_3 & y_0 & y_1 \\ x_3 & y_3 & y_0 & y_1 & y_2 \\ \hline & r_0 & r_1 & r_2 & r_3 \end{array} \qquad \begin{array}{c|cccc} y_0 & x_0 & x_3 & x_2 & x_1 \\ y_1 & x_1 & x_0 & x_3 & x_2 \\ y_2 & x_2 & x_1 & x_0 & x_3 \\ y_3 & x_3 & x_2 & x_1 & x_0 \\ \hline & r_0 & r_1 & r_2 & r_3 \end{array}.$$

Далее будет использоваться именно это представление.

Рассматривается циклическая (или еще известная как арифметическая) свертка, поэтому слово «циклическая» в дальнейшем опускается.

Операторы E, O, L, U (*E-Even* (четный), *O-Odd* (нечетный), *L-Lower* (нижний), *U-Upper* (верхний)) определим следующим образом:

$$(E\overline{x})_k = x_{2k}\,,\ (O\overline{x})_k = x_{2k+1}\,, (L\overline{x})_k = x_k\,, (U\overline{x})_k = x_{N/2+k}\,,\ k = \overline{0, N/2-1}\,.$$

Циклический сдвиг влево элементов обозначим через $\overline{z} = (\overline{v})'$:

$$z_k = v_{(k+1) \bmod N}\,,\ k = \overline{0, N-1}\,.$$

Циклический сдвиг вправо элементов обозначим через $\overline{z} = (\overline{v})''$:

$$z_k = v_{(k+N-1) \bmod N}\,,\ k = \overline{0, N-1}\,.$$

Проиллюстрируем вид операторов для случая $N = 8$:

$$E\overline{x} = \begin{bmatrix} x_0 \\ x_2 \\ x_4 \\ x_6 \end{bmatrix},\quad O\overline{x} = \begin{bmatrix} x_1 \\ x_3 \\ x_5 \\ x_7 \end{bmatrix},\quad L\overline{x} = \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix},\quad U\overline{x} = \begin{bmatrix} x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix},\quad (E\overline{y})' = \begin{bmatrix} y_2 \\ y_4 \\ y_6 \\ y_0 \end{bmatrix},\quad (E\overline{y})'' = \begin{bmatrix} y_6 \\ y_0 \\ y_2 \\ y_4 \end{bmatrix}.$$

Циклический сдвиг влево элементов *n* раз обозначим через $\overline{z} = \left((\overline{v})'\right)^n$.

Циклический сдвиг вправо элементов *n* раз обозначим через $\overline{z} = \left((\overline{v})''\right)^n$.

Метод парисекции

Рассмотрим метод, предложенный Питасси [3] и обобщенный Девисом [6].

Лемма 1 [3]. Входящие и исходящие последовательности свертки $\overline{r} = \overline{x} \otimes \overline{y}$ могут быть расщеплены на равные группы в соответствии с четностью элементов последовательностей:

$$E\overline{r} = E\overline{x} \otimes E\overline{y} + O\overline{x} \otimes O\overline{y},$$
$$O\overline{r} = E\overline{x} \otimes O\overline{y} + O\overline{x} \otimes \left(E\overline{y}\right)'. \qquad (1)$$

y_0	x_0	x_7	x_6	x_5	x_4	x_3	x_2	x_1
y_1	x_1	x_0	x_7	x_6	x_5	x_4	x_3	x_2
y_2	x_2	x_1	x_0	x_7	x_6	x_5	x_4	x_3
y_3	x_3	x_2	x_1	x_0	x_7	x_6	x_5	x_4
y_4	x_4	x_3	x_2	x_1	x_0	x_7	x_6	x_5
y_5	x_5	x_4	x_3	x_2	x_1	x_0	x_7	x_6
y_6	x_6	x_5	x_4	x_3	x_2	x_1	x_0	x_7
y_7	x_7	x_6	x_5	x_4	x_3	x_2	x_1	x_0
	r_0	r_1	r_2	r_3	r_4	r_5	r_6	r_7

Рисунок 1 – Вычисление свертки для $N = 8$ стандартным методом

	y_0	x_0	x_6	x_4	x_2	x_7	x_5	x_3	x_1
Ey	y_2	x_2	x_0	x_6	x_4	x_1	x_7	x_5	x_3
	y_4	x_4	x_2	x_0	x_6	x_3	x_1	x_7	x_5
	y_6	x_6	x_4	x_2	x_0	x_5	x_3	x_1	x_7
	y_1	x_1	x_7	x_5	x_3	x_0	x_6	x_4	x_2
Oy	y_3	x_3	x_1	x_7	x_5	x_2	x_0	x_6	x_4
	y_5	x_5	x_3	x_1	x_7	x_4	x_2	x_0	x_6
	y_7	x_7	x_5	x_3	x_1	x_6	x_4	x_2	x_0
		r_0	r_2	r_4	r_6	r_1	r_3	r_5	r_7
			Er				Or		

Рисунок 2 – Вычисление свертки для $N = 8$ методом парисекции

Из выражений:

$$\overline{a} = (E\overline{x} + O\overline{x}) \otimes (E\overline{y} + O\overline{y}),$$
$$\overline{b} = (E\overline{x} - O\overline{x}) \otimes (E\overline{y} - O\overline{y}), \qquad E\overline{r} = 1/2(\overline{a} + \overline{b}),$$
$$\overline{c} = O\overline{x} \otimes \left[\left(E\overline{y}\right)' - E\overline{y}\right], \qquad O\overline{r} = 1/2(\overline{a} - \overline{b}) + \overline{c} \qquad (2)$$

можно получить соотношения (1). С более детальным выводом формул (2) можно ознакомиться в [3].

Перейдем к вычислению свертки разрядностью $N = 2K$, где K – нечетное. Рассмотрим пример свертки разрядностью $N = 6 = 2 \cdot 3$:

y_0	x_0	x_5	x_4	x_3	x_2	x_1
y_1	x_1	x_0	x_5	x_4	x_3	x_2
y_2	x_2	x_1	x_0	x_5	x_4	x_3
y_3	x_3	x_2	x_1	x_0	x_5	x_4
y_4	x_4	x_3	x_2	x_1	x_0	x_5
y_5	x_5	x_4	x_3	x_2	x_1	x_0
	r_0	r_1	r_2	r_3	r_4	r_5

Рисунок 3 – Вычисление свертки для $N = 6$ стандартным методом

	y_0	x_0	x_4	x_2	x_5	x_3	x_1
$E\overline{y}$	y_2	x_2	x_0	x_4	x_1	x_5	x_3
	y_4	x_4	x_2	x_0	x_3	x_1	x_5
	y_1	x_1	x_5	x_3	x_0	x_4	x_2
$O\overline{y}$	y_3	x_3	x_1	x_1	x_2	x_0	x_4
	y_5	x_5	x_3	x_5	x_4	x_2	x_0
		r_0	r_2	r_4	r_1	r_3	r_5
			$E\overline{r}$			$O\overline{r}$	

Рисунок 4 – Вычисление свертки для $N = 6$ методом парисекции

Воспользуемся тем свойством свертки нечетной разрядности, что циклический сдвиг нечетное число раз в одном направлении дает результат четного сдвига в другом направлении.

$$\overline{d} = \left[E\overline{x} + \left(O\overline{x}\right)' \right] \otimes \left[E\overline{y} + \left(O\overline{y}\right)' \right],$$

$$\overline{e} = \left[E\overline{x} - \left(O\overline{x}\right)' \right] \otimes \left[E\overline{y} - \left(O\overline{y}\right)' \right]. \qquad (3)$$

$$E\overline{r} = 1/2\left(\overline{d} + \overline{e}\right) = E\overline{x} \otimes E\overline{y} + \left(O\overline{x}\right)' \otimes \left(O\overline{y}\right)' = E\overline{x} \otimes E\overline{y} + O\overline{x} \otimes O\overline{y}, \qquad (4)$$

$$O\overline{r} = 1/2\left(\overline{d} - \overline{e}\right)'' = \left[E\overline{x} \otimes \left(O\overline{y}\right)' + \left(O\overline{x}\right)' \otimes E\overline{y} \right]'' = E\overline{x} \otimes O\overline{y} + O\overline{x} \otimes \left(E\overline{y}\right)'. \qquad (5)$$

Лемма 2. Имеют место соотношения:

$$\left(O\overline{x}\right)' \otimes \left(O\overline{y}\right)' = O\overline{x} \otimes O\overline{y},$$

$$E\overline{x} \otimes \left(O\overline{y}\right)' = \left(E\overline{x} \otimes O\overline{y}\right)', \qquad (6)$$

$$O\overline{x} \otimes \left(E\overline{y}\right)'' = \left(O\overline{x}\right)' \otimes E\overline{y}. \qquad (7)$$

Рассмотрим последовательно каждое соотношение на примере $N = 6$.

Начнем с $\left(O\overline{x}\right)' \otimes \left(O\overline{y}\right)' = O\overline{x} \otimes O\overline{y}$.

	y_1	x_1	x_5	x_3
$O\overline{y}$	y_3	x_3	x_1	x_5
	y_5	x_5	x_3	x_1
		z_0	z_2	z_4
			$E\overline{z}$	

$E\overline{z} = O\overline{x} \otimes O\overline{y}$

	y_3	x_3	x_1	x_5
$\left(O\overline{y}\right)'$	y_5	x_5	x_3	x_1
	y_1	x_1	x_5	x_3
		z_0	z_2	z_4
			$E\overline{z}$	

$E\overline{z} = \left(O\overline{x}\right)' \otimes \left(O\overline{y}\right)'$

Теперь рассмотрим $E\overline{x} \otimes \left(O\overline{y}\right)' = \left(E\overline{x} \otimes O\overline{y}\right)'$.

	y_1	x_0	x_4	x_2
$O\overline{y}$	y_3	x_2	x_0	x_4
	y_5	x_4	x_2	x_0
		z_1	z_3	z_5
			$O\overline{z}$	

$O\overline{z} = E\overline{x} \otimes O\overline{y}$

	y_3	x_0	x_4	x_2
$\left(O\overline{y}\right)'$	y_5	x_2	x_0	x_4
	y_1	x_4	x_2	x_0
		z_3	z_5	z_1
			$\left(O\overline{z}\right)'$	

$\left(O\overline{z}\right)' = E\overline{x} \otimes \left(O\overline{y}\right)'$

Аналогично можно показать, что $O\overline{x} \otimes \left(E\overline{y}\right)'' = \left(O\overline{x} \otimes E\overline{y}\right)''$.

Из (6) следует, что: $\left(E\overline{x} \otimes \left(O\overline{y}\right)' \right)'' = \left(\left(E\overline{x} \otimes O\overline{y}\right)' \right)'' = E\overline{x} \otimes O\overline{y}$.

В заключении рассмотрим $O\overline{x} \otimes \left(E\overline{y}\right)'' = \left(O\overline{x}\right)' \otimes E\overline{y}$.

	y_0	x_1	x_5	x_3
$E\overline{y}$	y_2	x_3	x_1	x_5
	y_4	x_5	x_3	x_1
		z_1	z_3	z_5
			$O\overline{z}$	

$O\overline{z} = O\overline{x} \otimes E\overline{y}$

	y_4	x_1	x_5	x_3
$\left(E\overline{y}\right)''$	y_0	x_3	x_1	x_5
	y_2	x_5	x_3	x_1
		z_5	z_1	z_3
			$\left(O\overline{z}\right)''$	

$\left(O\overline{z}\right)'' = O\overline{x} \otimes \left(E\overline{y}\right)''$

	y_0	x_3	x_1	x_5
$E\overline{y}$	y_2	x_5	x_3	x_1
	y_4	x_1	x_5	x_3
		z_5	z_1	z_3
			$\left(O\overline{z}\right)''$	

$\left(O\overline{z}\right)'' = \left(O\overline{x}\right)' \otimes E\overline{y}$

Аналогично можно показать, что верно соотношение $\left(O\overline{x}\right)'' \otimes E\overline{y} = O\overline{y} \otimes \left(E\overline{x}\right)'$.

С учетом формул (6), (7) соотношение (5) примет вид:

$$\left(\left(O\overline{x}\right)' \otimes E\overline{y}\right)'' = \left(O\overline{x}\right)' \otimes \left(E\overline{y}\right)'' = O\overline{x} \otimes \left(\left(E\overline{y}\right)''\right)^2 . \qquad (8)$$

С учетом того, что два циклических сдвига вправо можно заменить одним сдвигом влево, соотношение в формуле (8) примет вид:

$$O\overline{x} \otimes \left(\left(E\overline{y}\right)''\right)^2 = O\overline{x} \otimes \left(E\overline{y}\right)' .$$

Продемонстрируем более подробно, в чем состоит предложенный метод.

$E\overline{y}$	y_0	x_0	x_4	x_2	x_5	x_3	x_1
	y_2	x_2	x_0	x_4	x_1	x_5	x_3
	y_4	x_4	x_2	x_0	x_3	x_1	x_5
$O\overline{y}$	y_1	x_1	x_5	x_3	x_0	x_4	x_2
	y_3	x_3	x_1	x_1	x_2	x_0	x_4
	y_5	x_5	x_3	x_5	x_4	x_2	x_0
		r_0	r_2	r_4	r_1	r_3	r_5
			$E\overline{r}$			$O\overline{r}$	

Рисунок 5 – Вычисление свертки методом парисекции

$E\overline{y}$	y_0	x_0	x_4	x_2	x_3	x_1	x_5
	y_2	x_2	x_0	x_4	x_5	x_3	x_1
	y_4	x_4	x_2	x_0	x_1	x_5	x_3
$\left(O\overline{y}\right)'$	y_3	x_3	x_1	x_5	x_0	x_4	x_2
	y_5	x_5	x_3	x_1	x_2	x_0	x_4
	y_1	x_1	x_5	x_3	x_4	x_2	x_0
		r_0	r_2	r_4	r_3	r_5	r_1
			$E\overline{r}$			$\left(O\overline{r}\right)'$	

Рисунок 6 – Вычисление свертки предложенным методом

Из рисунков видно, что результат совпадает. Так, например, при использовании обоих методов r_1 равно:

$$r_1 = y_0x_5 + y_2x_1 + y_4x_3 + y_3x_2 + y_5x_4 + y_1x_0 ,$$

$$r_1 = x_0y_1 + x_1y_2 + x_2y_3 + x_3y_4 + x_4y_5 + x_5y_0 ,$$

$$r_1 = \sum_{i=0}^{5} x_i \cdot y_{(i+1) \bmod 6} .$$

Видно, что в методе парисекции (рис. 5) нужно делать циклический сдвиг только в векторе $\left(Ox\right)''$, тогда как в предложенном методе, согласно соотношению (3), нужно циклически сдвигать в противоположную сторону оба вектора $\left(O\overline{x}\right)'$, $\left(O\overline{y}\right)'$ перед вычислением свертки. Из рис. 6 также видно, что для получения корректного результата нужно сдвинуть вектор $\left(\left(O\overline{r}\right)'\right)'' = O\overline{r}$.

Предложенный метод требует больше пред- и поствычислений в виде циклических сдвигов, но позволяет вычислить свертку за счет только 2 сверток меньшей размерности вместо 3 согласно стандартному методу парисекции.

Достаточно 10 умножений для вычисления свертки разрядностью $N = 5$ [2] и соответственно 20 умножений для вычисления свертки разрядностью $N = 10 = 2 \cdot 5$.

В этом случае формулы (3) – (5) примут вид:

$$\overline{d} = \left[E\overline{x} + \left(\left(O\overline{x} \right)' \right)^2 \right] \otimes \left[E\overline{y} + \left(\left(O\overline{y} \right)' \right)^2 \right],$$

$$\overline{e} = \left[E\overline{x} - \left(\left(O\overline{x} \right)' \right)^2 \right] \otimes \left[E\overline{y} - \left(\left(O\overline{y} \right)' \right)^2 \right],$$

$$E\overline{r} = 1/2\left(\overline{d} + \overline{e} \right),$$

$$O\overline{r} = 1/2\left(\left(\overline{d} - \overline{e} \right)'' \right)^2 .$$

Из формул видно, что нужно сдвинуть нечетные элементы на 2 позиции.

	y_0	x_0	x_8	x_6	x_4	x_2	x_9	x_7	x_5	x_3	x_1
	y_2	x_2	x_0	x_8	x_6	x_4	x_1	x_9	x_7	x_5	x_3
$E\overline{y}$	y_4	x_4	x_2	x_0	x_8	x_6	x_3	x_1	x_9	x_7	x_5
	y_6	x_6	x_4	x_2	x_0	x_8	x_5	x_3	x_1	x_9	x_7
	y_8	x_8	x_6	x_4	x_2	x_0	x_7	x_5	x_3	x_1	x_9
	y_1	x_1	x_9	x_7	x_5	x_3	x_0	x_8	x_6	x_4	x_2
	y_3	x_3	x_1	x_9	x_7	x_5	x_2	x_0	x_8	x_6	x_4
$O\overline{y}$	y_5	x_5	x_3	x_1	x_9	x_7	x_4	x_2	x_0	x_8	x_6
	y_7	x_7	x_5	x_3	x_1	x_9	x_6	x_4	x_2	x_0	x_8
	y_9	x_9	x_7	x_5	x_3	x_1	x_8	x_6	x_4	x_2	x_0
		r_0	r_2	r_4	r_6	r_8	r_1	r_3	r_5	r_7	r_8
				$E\overline{r}$					$O\overline{r}$		

Рисунок 7 – Вычисление свертки разрядностью $N = 10$ методом парисекции

Продемонстрируем, что, используя всего две матрицы меньшей разрядности,

$$E\overline{x} = \begin{bmatrix} x_0 & x_8 & x_6 & x_4 & x_2 \\ x_2 & x_0 & x_8 & x_6 & x_4 \\ x_4 & x_2 & x_0 & x_8 & x_6 \\ x_6 & x_4 & x_2 & x_0 & x_8 \\ x_8 & x_6 & x_4 & x_2 & x_0 \end{bmatrix} \qquad \left(\left(O\overline{x} \right)' \right)^2 = \begin{bmatrix} x_5 & x_3 & x_1 & x_9 & x_7 \\ x_7 & x_5 & x_3 & x_1 & x_9 \\ x_9 & x_7 & x_5 & x_3 & x_1 \\ x_1 & x_9 & x_7 & x_5 & x_3 \\ x_3 & x_1 & x_9 & x_7 & x_5 \end{bmatrix}$$

можно представить свертку разрядностью $N = 10 = 2 \cdot 5$:

	y_0	x_0	x_8	x_6	x_4	x_2	x_5	x_3	x_1	x_9	x_7
	y_2	x_2	x_0	x_8	x_6	x_4	x_7	x_5	x_3	x_1	x_9
$E\overline{y}$	y_4	x_4	x_2	x_0	x_8	x_6	x_9	x_7	x_5	x_3	x_1
	y_6	x_6	x_4	x_2	x_0	x_8	x_1	x_9	x_7	x_5	x_3
	y_8	x_8	x_6	x_4	x_2	x_0	x_3	x_1	x_9	x_7	x_5
	y_5	x_5	x_3	x_1	x_9	x_7	x_0	x_8	x_6	x_4	x_2
	y_7	x_7	x_5	x_3	x_1	x_9	x_2	x_0	x_8	x_6	x_4
$\left(\left(O\overline{y} \right)' \right)^2$	y_9	x_9	x_7	x_5	x_3	x_1	x_4	x_2	x_0	x_8	x_6
	y_1	x_1	x_9	x_7	x_5	x_3	x_6	x_4	x_2	x_0	x_8
	y_3	x_3	x_1	x_9	x_7	x_5	x_8	x_6	x_4	x_2	x_0
		r_0	r_2	r_4	r_6	r_8	r_5	r_7	r_9	r_1	r_3
				$E\overline{r}$					$\left(\left(O\overline{r} \right)' \right)^2$		

Количество сдвигов равно $n = \lfloor K/2 \rfloor$, где K – нечетное число и множитель разрядности свертки $N = 2K$.

Теперь можно выразить в общем виде формулы для вычисления свертки разрядностью $N = 2K$, где K – нечетное число.

$$\overline{d} = \left[E\overline{x} + \left(\left(O\overline{x} \right)' \right)^n \right] \otimes \left[E\overline{y} + \left(\left(O\overline{y} \right)' \right)^n \right],$$

$$\overline{e} = \left[E\overline{x} - \left(\left(O\overline{x} \right)' \right)^n \right] \otimes \left[E\overline{y} - \left(\left(O\overline{y} \right)' \right)^n \right],$$

$$E\overline{r} = 1/2\left(\overline{d} + \overline{e}\right), O\overline{r} = 1/2\left(\left(\overline{d} - \overline{e} \right)'' \right)^n .$$

Покажем практическое применение свертки для вычисления операции умножения многоразрядных чисел, которая широко используется при реализации алгоритмов асимметричной криптографии. Покажем вначале на примере свертки разрядностью 2*К*, где *К* – четное.

Умножение двух чисел $\overline{x} = (x_0, x_1, x_2, x_3), \overline{y} = (y_0, y_1, y_2, y_3)$ разрядностью 4 с использованием свертки можно представить в виде:

$$\overline{r} = (x_0, x_1, x_2, x_3, 0,0,0,0) \otimes (0,0,0,0, y_3, y_2, y_1, y_0).$$

x_0	0	0	0	0	y_3	y_2	y_1	y_0
x_1	0	0	0	y_3	y_2	y_1	y_0	0
x_2	0	0	y_3	y_2	y_1	y_0	0	0
x_3	0	y_3	y_2	y_1	y_0	0	0	0
0	y_3	y_2	y_1	y_0	0	0	0	0
0	y_2	y_1	y_0	0	0	0	0	y_3
0	y_1	y_0	0	0	0	0	y_3	y_2
0	y_0	0	0	0	0	y_3	y_2	y_1
	r_7	r_6	r_5	r_4	r_3	r_2	r_1	r_0

Рисунок 8 – Вычисление свертки стандартным методом при реализации операции умножения двух чисел разрядностью 4

x_0	0	0	0	0	y_3	y_2	y_1	y_0
x_1	0	0	0	y_3	y_2	y_1	y_0	0
x_2	0	0	y_3	y_2	y_1	y_0	0	0
x_3	0	y_3	y_2	y_1	y_0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
	r_7	r_6	r_5	r_4	r_3	r_2	r_1	r_0

Рисунок 9 – Вычисление свертки стандартным методом при реализации операции умножения двух чисел разрядностью 4 с учетом нулевых элементов

Окончательно получаем:

x_0					y_3	y_2	y_1	y_0
x_1				y_3	y_2	y_1	y_0	
x_2			y_3	y_2	y_1	y_0		
x_3		y_3	y_2	y_1	y_0			
	r_7	r_6	r_5	r_4	r_3	r_2	r_1	r_0

Рисунок 10 – Умножение двух чисел с использование свертки без нулевых элементов

				y_3	y_2	y_1	y_0
				x_3	x_2	x_1	x_0
				x_0y_3	x_0y_2	x_0y_1	x_0y_0
			x_1y_3	x_1y_2	x_1y_1	x_1y_0	
		x_2y_3	x_2y_2	x_2y_1	x_2y_0		
	x_3y_3	x_3y_2	x_3y_1	x_3y_0			
r_7	r_6	r_5	r_4	r_3	r_2	r_1	r_0

Рисунок 11 – Умножение двух чисел в столбик

Из рис. 10 и 11 видно, что использованная таким образом свертка реализует стандартный метод умножения в столбик, за исключением того, что результат получается в обратном порядке.

Приведем пошаговое описание алгоритма реализации операции умножения *K*-разрядных чисел с использованием свертки:

Шаг 1. $a_i = x_i$, $i = \overline{0, K-1}$, $a_i = 0$, $i = \overline{K, N-1}$.

Шаг 2. $b_i = 0$, $i = \overline{0, K-1}$, $b_i = y_{N-1-i}$, $i = \overline{K, N-1}$.

Шаг 3. $\overline{r} = \overline{a} \otimes \overline{b}$.

Шаг 4. $w_i = r_{N-1-i}$, $i = \overline{0, N-1}$.

Вектор $\overline{w}$ разрядностью $N = 2K$ будет содержать результат операции умножения чисел, представленных в виде вектров $\overline{x}$ и $\overline{y}$ разрядностью *K*.

Данный алгоритм справедлив и для сверток рязрядностью $N = 2K$, где *K* – нечетное.

Заметим, что для вычисления операции умножения *K*-разрядных чисел с использованием алгоритма быстрого преобразования Фурье необходимо вычислять циклическую свертку также с разрядностью 2*K*. Это связано с тем, что при умножении двух *K*-разрядных чисел, результат умножения получается разрядностью 2*K*.

Количество операций умножения при вычислении свертки разрядностью $N = 2^n$, $n > 2$ методом парисекции выражается следующим соотношением:

$$M_N = 5 \cdot 3^{n-2}, \tag{9}$$

где *M* – количество операций умножения, *N* – разрядность свертки.

Количество операций умножения *M* при вычислении свертки большой разрядности вида $N = K \cdot 2^n$, $n > 1$, где *K* – нечетное, приведено ниже в виде таблицы.

Таблица 1

Значение *K* в (9)	Количество операций умножения M_K для вычисления свертки разрядности *K*	Разрядность свертки $N = K \cdot 2^n$, $n > 1$	Количество операций умножения *M* при вычислении свертки разрядности $N = K \cdot 2^n, n > 1$
3	4	$N = 3 \cdot 2^n$	$M = 8 \cdot 3^{n-1}$
5	10	$N = 5 \cdot 2^n$	$M = 20 \cdot 3^{n-1}$
7	16	$N = 7 \cdot 2^n$	$M = 32 \cdot 3^{n-1}$
9	19	$N = 9 \cdot 2^n$	$M = 38 \cdot 3^{n-1}$

Из табл. 1 видно, что можно конструировать свертки размерностью, отличной от $N = 2^n$, $n > 2$, что является одним из преимуществ предложенного метода. Вторым преимуществом является то, что в некоторых случаях эффективнее использовать свертку большей разрядности вида $N = K \cdot 2^n$, $n > 1$, где *K* – нечетное, вместо

свертки разрядностью $N = 2^n$, $n > 2$. Так, например, для вычисления свертки разрядности $N = 18$ требуется всего 38 умножений согласно таблице, тогда как для вычисления свертки $N = 16$ методом парисекции необходимо 45 умножений по формуле (9).

Заключение

В данной работе приведен эффективный метод вычисления свертки разрядностью 2*K*, где *K* – нечетное. В общем виде приведены формулы вычисления циклической свертки разрядностью 2*K*, где *K* – нечетное. Приведен алгоритм реализации операции умножения с использованием циклической свертки. В виде таблицы приведены оценки сложности вычисления свертки большой разрядности вида $N = K \cdot 2^n$, $n > 1$, где $K = 3,5,7,9$.

Литература

1. Задірака В.К., Олексюк О.С. Комп'ютерна арифметика багаторозрядних чисел. – К.: Наук. думка, 2003. – 263 с.
2. Нуссбаумер Г. Быстрое преобразование Фурье и алгоритмы вычисления сверток: Пер. с англ. – М: Радио и связь, 1985. – С. 66.
3. Pitassi D.A. Fast convolution using the Walsh transform // Applicat. Walsh Functions. – 1971. – Apr. – P. 130-133.
4. Ахмед Н., Рао К.Р. Ортогональные преобразования при обработке цифровых сигналов. – М.: Связь, 1980. – 248 с.
5. Хармут Х. Теория секветного анализа: Основы и применение. – М.: Мир, 1980. – 574.
6. Davis W.F. A class of efficient convolution algorithms // Applicat. Walsh Functions. – 1972. – March. – P. 318-329.

А.М. Терещенко

Оптимізація методу Пітассі обчислення згортки

Запропонований метод розширює діапазон використовуваних розрядностей циклічної згортки за рахунок застосування ефективного методу обчислення циклічної згортки розрядністю 2*K*, де *K* – непарне. Показано, що для обчислення згортки такої розрядності достатньо обчислити тільки дві згортки половинної (від начальної) розрядності, при більшій кількості перед- та постобчислень у вигляді циклічних зсувів. Представлені в загальному вигляді формули обчислення циклічної згортки. Наведена реалізації операції багаторозрядного множення на основі циклічної згортки. У вигляді таблиці наведені оцінки складності обчислення циклічної згортки великої розрядності виду $N = K \cdot 2^n$, $n > 1$ для $K = 3,5,7,9$.

A.N. Tereshcenko

The suggested method extends the range of used measurements of cyclic convolutions with using of effective calculation method of cyclic convolutions with measurement 2*K* then *K* is odd. It is shown for convolution calculation with that measurement it is enough to calculate only 2 convolutions half-measurement with more number of pre- and post-calculations like cyclic shifts. It is given in general the calculation formulas of cyclic convolution. It is given the building of multi-digit multiplication with using cyclic convolution. The complexities of cyclic convolution calculation with measurement $N = K \cdot 2^n$, $n > 1$ for $K = 3,5,7,9$. are given in table.

Статья поступила в редакцию 21.07.2008.